CLAIMS

Please amend the claims as follows:

1. (currently amended) A method for managing a user key used to sign a message for a data processing system, said method comprising:

assigning a user key to a user and storing the user key in an encrypting data processing system utilized to encrypt messages;

encrypting the messages with the user key;

storing an associated key in the encrypting data processing system and encrypting the user key with the associated key to obtain an encrypted user key, wherein said associated key comprises a key that is not publicly published;

said encrypting data processing system communicating at least one encrypted message together with the encrypted user key to a recipient system in order to permit validation of an association of the user with the encrypted messages by the recipient system; and

thereafter, preventing validation of the association of the user with messages by revoking the associated key at the encrypting data processing system so that the encrypting data processing system is no longer able to decrypt the encrypted user key.

2. (original) The method according to Claim 1, further comprising:

decrypting the user key with the associated key; and

decrypting the messages with the user key.

3. (previously presented) The method according to Claim 1, wherein:

the encrypting data processing system further comprises a client system and a server system coupled for communication, said client system having a client memory device and said server system having an encryption chip and a server memory device;

storing the user key further comprises storing the user key in the client memory device;

storing the associated key further comprises storing the associated key in the server memory device; and

preventing validation further comprises preventing validation of messages associated with the user by eliminating the associated key from the server memory device.

4. (original) The method according to Claim 3, wherein encrypting the messages further comprises:

sending the messages to be encrypted from the client system to the server system;

encrypting the messages using the encryption chip of the server system; and

sending the encrypted messages from the server system to the client system.

5. (original) The method according to Claim 4, further comprising:

erasing from the server system all data relating to the encrypted messages after the encrypted messages are sent from the server system to the client system.

6. (previously presented) The method according to Claim 1, further comprising:

encrypting the associated key by using an encryption chip key which is stored on an encryption chip of the encrypting data processing system.

7. (previously presented) The method according to Claim 6, further comprising:

communicating an encrypted associated key to validate the association of the user with the encrypted messages.

8. (original) The method according to Claim 7, further comprising:

decrypting the associated key with the encryption chip key.

9. (currently amended) A system for managing a user key used to sign a message, said system comprising:

means for assigning a user key to a user;

means for storing the user key;

means for encrypting the messages with the user key;

means for storing an associated key;

means for encrypting the user key with the associated key to obtain an encrypted user key, wherein said associated key comprises a key that is not publicly published;

means for communicating at least one encrypted message together with the encrypted user key to a recipient system in order to permit validation of an association of the user with the encrypted messages by the recipient system; and

means for thereafter preventing validation of the association of the user with messages by revoking the associated key in said system so that the encrypting data processing system is no longer able to decrypt the encrypted user key.

10. (original) The system according to Claim 9, further comprising:

means for decrypting the user key with the associated key; and

means for decrypting the messages with the user key.

11. (previously presented) The system according to Claim 9, wherein:

the system further comprises a client system and a server system coupled together for communication, said client system having a client memory device and said server system having an encryption chip and a server memory device;

said means for storing the user key further comprises means for storing the user key in the client memory device;

said means for storing the associated key further comprises means for storing the associated key in the server memory device; and

said means for preventing validation further comprises means for preventing the validation of messages associated with the user by eliminating the associated key from the server memory device.

12. (original) The system according to Claim 11, wherein said means for encrypting the messages further comprises:

means for sending the messages to be encrypted from the client system to the server system;

means for encrypting the messages using the encryption chip of the server system; and

means for sending the encrypted messages from the server system to the client system.

13. (original) The system according to Claim 12, further comprising:

means for erasing from the server system all data relating to the encrypted messages after the encrypted messages are sent from the server system to the client system.

14. (previously presented) The system according to Claim 9, further comprising:

an encryption chip that encrypts the associated key by using an encryption chip key stored within the encryption chip.

15. (previously presented) The system according to Claim 14, further comprising:

means for communicating an encrypted associated key to validate the association of the user with the encrypted messages.

16. (original) The system according to Claim 15, further comprising:

means for decrypting the associated key with the encryption chip key.

17. (currently amended) A program product for managing a user key used to sign a message, said program product comprising:

a control program including:

instruction means for assigning a user key to a user and for storing the user key in an encrypting data processing system utilized to encrypt messages;

instruction means for encrypting the messages with the user key;

instruction means for storing an associated key in the encrypting data processing system and for encrypting the user key with the associated key to obtain an encrypted user key, wherein said associated key comprises a key that is not publicly published;

instruction means for communicating at least one encrypted message together with the encrypted user key to a recipient system in order to permit validation of an association of the user with the encrypted messages by the recipient system;

instruction means for thereafter preventing validation of the association of the user with messages by revoking the associated key within the encrypting data processing

system so that the encrypting data processing system is no longer able to decrypt the encrypted user key; and

computer usable media bearing said control program.

18. (original) The program product according to Claim 17, further comprising:

instruction means for decrypting the user key with the associated key; and

instruction means for decrypting the messages with the user key.

19. (previously presented) The program product according to Claim 17, wherein:

the encrypting data processing system further comprises a client system and a server system coupled together for communication, said client system having a client memory device and said server system having an encryption chip and a server memory device;

said instruction means for storing the user key further comprises instruction means for storing the user key in the client memory device;

said instruction means for storing the associated key further comprises instruction means for storing the associated key in the server memory device; and

said instruction means for preventing validation further comprises instruction means for preventing the validation of the messages associated with the user by eliminating the associated key from the server memory device.

20. (original) The program product according to Claim 19, wherein said instruction means for encrypting the messages further comprises:

instruction means for sending the messages to be encrypted from the client system to the server system;

instruction means for encrypting the messages using the encryption chip of the server system; and

instruction means for sending the encrypted messages from the server system to the client system.

21. (original) The program product according to Claim 20, further comprising:

instruction means for erasing from the server system all data relating to the encrypted messages after the encrypted messages are sent from the server system to the client system.

22. (original) The program product according to Claim 17, further comprising:

instruction means for encrypting the associated key by using an encryption chip key which is stored on an encryption chip of the data processing system.

23. (previously presented) The program product according to Claim 22, further comprising:

instruction means for communicating an encrypted associated key to validate the association of the user with the encrypted messages.

24. (original) The program product according to Claim 23, further comprising:

instruction means for decrypting the associated key with the encryption chip key.